Notice of Allowability	**Application No.** 09/734,777	**Applicant(s)** STARING, ANTONIUS A.M.	
	Examiner Zachary A. Davis	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *The Request for Continued Examination received 14 February 2006*.

2. ☒ The allowed claim(s) is/are *1-12*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☒ All b) □ Some* c) □ None of the:

   1. ☒ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 17 January 2006 has been entered.

2. By the above submission, Claims 1, 3, 9, 10, and 11 have been amended. No claims were added or canceled. Claims 1-12 are currently pending in the present application.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Larry Liberchuk on 19 April 2006.

The application has been amended as follows:

IN THE CLAIMS:

Please **REPLACE Claims 1, 5, and 9-12** with the following amended claims.

1. A secure communication system including

a source device and

at least one sink device; information being transferred from the source device to the at least one sink device in a communication session including the transfer of a plurality of packets from the source device to the at least one sink device; each packet including a data field for transferring a portion of the information;

the source device including:

a key generator for, at the initiative of the source device, generating an active session source key in a predetermined sequence of source session keys Ksource$_i$;

an encryptor for encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field that contains a key check block such that a plain-text form of the key check block is a data block agreed between the source and sink devices before starting the transfer of the information;

the at least one sink device including:

a key generator for generating a plurality of candidate sink session ~~key~~ keys in a predetermined sequence of sink session keys $Ksink_i$, where for each index i in the sequence the respective sink session key $Ksink_i$ corresponds to the respective source session key $Ksource_i$;

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key;

a key resolver operative

to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found; and

to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

5. A secure communication system as claimed in claim 4, wherein

the source and sink ~~device~~ devices each include corresponding key check block generators for generating the plain-text form of the key check block and effecting the change of the plain-text form of the key check block.

9. A sink device for use in a secure communication system wherein a source device autonomously can change a source session key used for encrypting at least part of the data field of a packet transferred from the source device to the sink device; the encrypted part of the data field including a sub-field designated as a key check block field; the sink device including:

a key generator for generating a plurality of candidate sink session ~~key~~ keys in a predetermined sequence of sink session keys $Ksink_i$, where for each index i in the sequence the respective sink session key $Ksink_i$ corresponds to the respective source session key $Ksource_i$;

a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key; and

a key resolver operative

to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found, the key check block field containing a key check block such that a plain-text form of the key check block is a data block agreed between the source and sink devices before starting the transfer of the information; and

to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

10. A method of secure communication between a source device and at least one sink device; information being transferred from the source device to the at least one sink device in a communication session including the transfer of a plurality of packets from the source device to the at least one sink device; each packet including a data field for transferring a portion of the information; the method including:

at the initiative of the source device, generating an active session source key in a predetermined sequence of source session keys Ksource$_i$;

encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field that contains a key check block such that a plain-text form of the key check block is a data block agreed between the source and sink devices before starting the transfer of the information;

transferring the packet from the source device to the at least one sink device;

generating a plurality of candidate sink session ~~key~~ keys in a predetermined sequence of sink session keys Ksink$_i$, where for each index i in the sequence the respective sink session key Ksink$_i$ corresponds to the respective source session key Ksource$_i$;

determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by decrypting the data in the key check block field of the received packet under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found; and decrypting a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

11. A method of, in a sink device in a secure communication system, detecting a change of a session key effected by a source device in the system; information being transferred from the source device to the sink device in a communication session including the transfer of a plurality of packets from the source device to the sink device; each packet including a data field for transferring a portion of the information; at least part of the data field of a packet being encrypted under control of an active source session key in a predetermined sequence of source session keys Ksource$_i$; the encrypted part of the data field including a sub-field designated as a key check block field; the method including:

generating a plurality of candidate sink session ~~key~~ keys in a predetermined sequence of sink session keys Ksink$_i$, where for each index i in the sequence the respective sink session key Ksink$_i$ corresponds to the respective source session key Ksource$_i$;

determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of a different one of the plurality of candidate sink session keys until a valid decryption result is found, the key check block field containing a key check block such that a plain-text form of the key check block is a data block agreed between the source and sink devices before starting the transfer of the information; and

decrypting a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid decryption result.

12. A computer program product, stored in a computer readable medium, where the program product is operative to cause a computer to perform the method of claim 11.

Allowable Subject Matter

4. Claims 1-12 are allowed.

5. Reasons for allowance were set forth in the Office actions mailed 06 May 2004 and 13 January 2005. For convenience, a summary of those reasons appears below.

6. The following is an examiner's statement of reasons for allowance:

The independent Claims are directed to systems and methods in which encrypted data is transferred from a source to at least one sink device, and a sink device determines which key of a plurality of candidate keys is the appropriate key to decrypt the encrypted data. The determination is performed by decrypting a key check block with candidate keys until a valid result is found. The closest prior art, Komuro et al, US Patent 6223285, and Gray et al, US Patent 57063448, in combination also discloses secure systems that generate a sequence of session keys and determines which candidate key is the appropriate key to be used, based on a key check block. However, each of the independent Claims also recites that the plain-text of the key check block "is a data block agreed between the source and sink devices before starting the transfer of the information". Neither Komuro nor Grey, alone or in combination, teaches nor suggests this limitation. Therefore the claims are allowable over the cited prior art, as previously noted.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Fielder et al, US Patent 6105133, discloses a system that includes updating dynamic secrets using a pseudo-random change value.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER